CLAIMS

What is claimed is:

1. A method of providing client security for networked services, the method comprising the computer-implemented steps of:

storing a credential such that the credential is accessible only by using a local security authority;

generating a secret value corresponding to the credential; and

storing the secret value in a secret file that can be modified and retrieved only by a first user.

2. A method as recited in claim 1, further comprising:

receiving user information provided by the first user;

authenticating the first user based, at least in part, on the user information;

determining the credential based, at least in part, on the user information;

associating the credential with the first user; and

associating a credential identifier with the credential.

3. A method as recited in claim 2, wherein determining the credential includes using the local security authority to exchange information, including at least part of said user information, with a security server.

4. A method as recited in claim 2, wherein authenticating the first user includes exchanging information, representing at least a part of the user information, with a security server by using the local security authority.

5. A method as recited in claim 4, wherein exchanging information and determining the credential includes conducting a Kerberos exchange with a Kerberos security server whereby when information is passed from the local security authority to the Kerberos security server, the Kerberos security server determines the credential based, at least in part, on the information from the local security authority, and passes the credential to the local security authority.

6. A method as recited in claim 1, wherein generating and writing the secret value includes using the local security authority.

7. A method as recited in claim 2, further comprising:
receiving a request to retrieve the credential;
retrieving the secret value;
retrieving the credential identifier, using the secret value; and
retrieving the credential, using the credential identifier.

8. A method as recited in claim 7, further comprising:
passing the credential identifier from the local security authority to an application client;
receiving a request to initialize a security context;
obtaining authentication information by using the local security authority and using the credential;
passing the authentication information to a security library; and

passing the authentication information from the security library to the application client, thereby facilitating initialization of the security context, wherein retrieving the credential includes identifying the credential that corresponds to the secret value and to the credential identifier by using the local security authority.

9. A method as recited in claim 7, wherein the secret value is retrieved only if the request to retrieve the credential is received from the first user.

10. A method as recited in claim 1, further comprising:

retrieving the secret value from the secret file;

passing the secret value to the local security authority;

identifying the credential to which the secret value corresponds by using the local security authority to correlate a characteristic of the secret value with a characteristic of the credential;

obtaining authentication information from a security server, using the credential and the local security authority; and

passing authentication information from the local security authority to an application client, wherein the authentication information can operate with the application client to access a computer networked service.

11. A method as recited in claim 10, wherein retrieving and passing the secret value include using a security library to access the secret file, to read the secret value, and to communicate the secret value to the local security authority.

12. A method as recited in claim 10, wherein the method further comprises receiving user information provided by the first user; and wherein obtaining the authentication information includes exchanging information with the security server by using the local security authority to initiate communication with the security server, to pass at least part of the user information to the security server, and to receive authentication information from the security server.

13. A method as recited in claim 1, wherein the credential is associated with a first application and a set of permissions, and wherein the method further comprises:

storing a second credential associated with a second application, in memory associated with the local security authority, wherein the second credential is associated with a subset of the set of permissions;

generating a second secret value corresponding to the second credential;

storing the second secret value in a second secret file; and

limiting access to the second secret file to only the second application when invoked by the first user.

14. A method as recited in claim 13, further comprising:

receiving a request from the second application to retrieve the second credential;

retrieving the second secret value from the second secret file;

passing the second secret value to the local security authority;

confirming the request is from the second application;

identifying the second credential to which the second secret value corresponds by using the local security authority to correlate a characteristic of the second secret value with a characteristic of the second credential;

obtaining second authentication information from a security server, using the second credential and the local security authority; and

passing the second authentication information from the local security authority to a second application client, wherein the second authentication information can operate with the second application client to access a computer networked service.

15. A computer readable medium containing program instructions for limiting access to a credential that can facilitate access by a first user to a computer networked service on a networked computer system, wherein when the computer readable medium is read by a computer system having a processor and memory the program instructions are configured to be executed by the processor, the computer readable medium comprising:

program instructions for storing the credential such that the credential is accessible only by using a local security authority;

program instructions for generating a secret value corresponding to the credential; and

program instructions for storing the secret value in a secret file that can be modified and retrieved only by the first user.

16. A computer-readable medium as recited in claim 15, further comprising:

program instructions for recognizing user information provided by the first user;

program instructions for authenticating the first user based, at least in part, on the user information;

program instructions for determining the credential based, at least in part, on the user information;

program instructions for associating the credential with the first user; and

program instructions for associating a credential identifier with the credential.

17. A computer readable medium as recited in claim 16, wherein the program instructions for determining the credential include program instructions for using the local security authority to exchange information, including at least part of the user information, with a security server.

18. A computer readable medium as recited in claim 16, further comprising:

program instructions for recognizing a request to retrieve the credential;

program instructions for retrieving the secret value;

program instructions for retrieving the credential identifier, using the secret value; and

program instructions for retrieving the credential, using the credential identifier.

19. A computer readable medium as recited in claim 18, further comprising:

program instructions for passing the credential identifier from the local security authority to an application client;

program instructions for receiving a request to initialize a security context;

program instructions for obtaining authentication information by using the local security authority and using the credential;

program instructions for passing the authentication information to a security library; and

program instructions for passing the authentication information from the security library to the application client, thereby initializing the security context, wherein retrieving the credential includes identifying the credential that corresponds to the secret value and to the credential identifier, by using the local security authority.

20. A computer readable medium as recited in claim 15, further comprising:

program instructions for retrieving the secret value from the file;

program instructions for passing the secret value to the local security authority;

program instructions for identifying the credential to which the secret value corresponds, by using the local security authority to correlate a characteristic of the secret value with a characteristic of the credential;

program instructions for obtaining authentication information from a security server, using the credential and the local security authority; and

program instructions for passing authentication information from the local security authority to an application client, wherein the authentication information can operate with the application client to access the computer networked service.

21. A computer system configured to provide client security for networked services, the computer system comprising:

a local security authority configured to authenticate the identity of a user, to determine a credential corresponding to the user, to generate a secret value corresponding to the determined credential, and to determine authorization information associated with both the user and an application;

local security authority memory associated with the local security authority, configured only by operation of the local security authority; and

computer-readable memory configured to store a secret file which is configured to store the secret value and which is readable substantially only by processes executed by the user.

22. The computer system as recited in claim 21, further comprising:

an application client configured to request processes from an application server; and

a security library associated with the application client, wherein the security library is configured to receive a request from the application client to initiate a security context, to obtain the secret value by reading the secret file, to communicate the secret value to the local security authority, to obtain the authorization information from the local security authority, and to communicate the authorization information to the application client.

23. A computer system as recited in claim 21, wherein the local security authority is configured to authenticate the identity of the user, to determine the credential corresponding to the user, and to determine authorization information associated with both the user and an application by receiving user information and exchanging information, including information representing at least a part of the user information, with a security server.

24. An apparatus for providing client security for networked services, comprising:

a network interface that is coupled to a data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

storing a credential such that the credential is accessible only by using a local security authority;

generating a secret value corresponding to the credential; and

storing the secret value in a secret file that can be modified and retrieved only by a first user.

25. An apparatus as recited in Claim 24, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving user information provided by the first user;

authenticating the first user based, at least in part, on the user information;

determining the credential based, at least in part, on the user information;

associating the credential with the first user; and

associating a credential identifier with the credential.

26. An apparatus as recited in Claim 25, wherein determining the credential includes using the local security authority to exchange information, including at least part of said user information, with a security server.

27. An apparatus as recited in Claim 25, wherein authenticating the first user includes exchanging information, representing at least a part of the user information, with a security server by using the local security authority.

28. An apparatus as recited in Claim 27, wherein exchanging information and determining the credential includes conducting a Kerberos exchange with a Kerberos security server whereby when information is passed from the local security authority to the Kerberos security server, the Kerberos security server determines the credential based, at least in part, on the information from the local security authority, and passes the credential to the local security authority.

29. An apparatus as recited in Claim 24, wherein generating and writing the secret value includes using the local security authority.

30. An apparatus as recited in Claim 25, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:
receiving a request to retrieve the credential;
retrieving the secret value;
retrieving the credential identifier, using the secret value; and
retrieving the credential, using the credential identifier.

31. An apparatus as recited in Claim 30, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

passing the credential identifier from the local security authority to an application client;

receiving a request to initialize a security context;

obtaining authentication information by using the local security authority and using the credential;

passing the authentication information to a security library; and

passing the authentication information from the security library to the application client, thereby facilitating initialization of the security context, wherein retrieving the credential includes identifying the credential that corresponds to the secret value and to the credential identifier by using the local security authority.

32. An apparatus as recited in Claim 30, wherein the secret value is retrieved only if the request to retrieve the credential is received from the first user.

33. An apparatus as recited in Claim 24, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

retrieving the secret value from the secret file;

passing the secret value to the local security authority;

identifying the credential to which the secret value corresponds by using the local security authority to correlate a characteristic of the secret value with a characteristic of the credential;

obtaining authentication information from a security server, using the credential and the local security authority; and

passing authentication information from the local security authority to an application client, wherein the authentication information can operate with the application client to access a computer networked service.

34. An apparatus as recited in Claim 33, wherein retrieving and passing the secret value include using a security library to access the secret file, to read the secret value, and to communicate the secret value to the local security authority.

35. An apparatus as recited in Claim 33, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the step of receiving user information provided by the first user; and wherein obtaining the authentication information includes exchanging information with the security server by using the local security authority to initiate communication with the security server, to pass at least part of the user information to the security server, and to receive authentication information from the security server.

36. An apparatus as recited in Claim 24, wherein the credential is associated with a first application and a set of permissions, and wherein the apparatus further comprises one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

storing a second credential associated with a second application, in memory associated with the local security authority, wherein the second credential is associated with a subset of the set of permissions;

generating a second secret value corresponding to the second credential;

storing the second secret value in a second secret file; and

limiting access to the second secret file to only the second application when invoked by the first user.

37. An apparatus as recited in Claim 36, further comprising one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving a request from the second application to retrieve the second credential;

retrieving the second secret value from the second secret file;

passing the second secret value to the local security authority;

confirming the request is from the second application;

identifying the second credential to which the second secret value corresponds by using the local security authority to correlate a characteristic of the second secret value with a characteristic of the second credential;

obtaining second authentication information from a security server, using the second credential and the local security authority; and

passing the second authentication information from the local security authority to a second application client, wherein the second authentication information can operate with the second application client to access a computer networked service.

38. An apparatus providing client security for networked services, comprising:

means for storing a credential such that the credential is accessible only by using a local security authority;

means for generating a secret value corresponding to the credential; and

means for storing the secret value in a secret file that can be modified and retrieved only by a first user.

39. An apparatus as recited in Claim 38, further comprising:

means for receiving user information provided by the first user;

means for authenticating the first user based, at least in part, on the user information;

means for determining the credential based, at least in part, on the user information;

means for associating the credential with the first user; and

means for associating a credential identifier with the credential.

40. An apparatus as recited in Claim 39, wherein determining the credential includes using the local security authority to exchange information, including at least part of said user information, with a security server.

41. An apparatus as recited in Claim 39, wherein authenticating the first user includes exchanging information, representing at least a part of the user information, with a security server by using the local security authority.

42. An apparatus as recited in Claim 41, wherein exchanging information and determining the credential includes conducting a Kerberos exchange with a Kerberos

security server whereby when information is passed from the local security authority to the Kerberos security server, the Kerberos security server determines the credential based, at least in part, on the information from the local security authority, and passes the credential to the local security authority.

43. An apparatus as recited in Claim 38, wherein generating and writing the secret value includes using the local security authority.

44. An apparatus as recited in Claim 39, further comprising:
means for receiving a request to retrieve the credential;
means for retrieving the secret value;
means for retrieving the credential identifier, using the secret value; and
means for retrieving the credential, using the credential identifier.

45. An apparatus as recited in Claim 44, further comprising:
means for passing the credential identifier from the local security authority to an application client;
means for receiving a request to initialize a security context;
means for obtaining authentication information by using the local security authority and using the credential;
means for passing the authentication information to a security library; and
means for passing the authentication information from the security library to the application client, thereby facilitating initialization of the security context, wherein retrieving the credential includes identifying the credential that

corresponds to the secret value and to the credential identifier by using the local security authority.

46. An apparatus as recited in Claim 44, wherein the secret value is retrieved only if the request to retrieve the credential is received from the first user.

47. An apparatus as recited in Claim 38, further comprising:
means for retrieving the secret value from the secret file;
means for passing the secret value to the local security authority;
means for identifying the credential to which the secret value corresponds by using the local security authority to correlate a characteristic of the secret value with a characteristic of the credential;
means for obtaining authentication information from a security server, using the credential and the local security authority; and
means for passing authentication information from the local security authority to an application client, wherein the authentication information can operate with the application client to access the computer networked service.

48. An apparatus as recited in Claim 47, wherein retrieving and passing the secret value include using a security library to access the secret file, to read the secret value, and to communicate the secret value to the local security authority.

49. An apparatus as recited in Claim 47, further comprising a means for receiving user information provided by the first user; and wherein obtaining the authentication information includes exchanging information with the security server by using the

local security authority to initiate communication with the security server, to pass at least part of the user information to the security server, and to receive authentication information from the security server.

50. An apparatus as recited in Claim 38, wherein the credential is associated with a first application and a set of permissions, and wherein the apparatus further comprises:

means for storing a second credential associated with a second application, in memory associated with the local security authority, wherein the second credential is associated with a subset of the set of permissions;

means for generating a second secret value corresponding to the second credential;

means for storing the second secret value in a second secret file; and

means for limiting access to the second secret file to only the second application when invoked by the first user.

51. An apparatus as recited in Claim 50, further comprising:

means for receiving a request from the second application to retrieve the second credential;

means for retrieving the second secret value from the second secret file;

means for passing the second secret value to the local security authority;

means for confirming the request is from the second application;

means for identifying the second credential to which the second secret value corresponds by using the local security authority to correlate a characteristic of the second secret value with a characteristic of the second credential;

means for obtaining second authentication information from a security server, using the second credential and the local security authority; and

means for passing the second authentication information from the local security authority to a second application client, wherein the second authentication information can operate with the second application client to access a computer networked service.